A New Form of Warfare? Implications of the Cyber Attack on Sony

> This blog post was first posted to the International Centre for Security Analysis blog on the 22nd January 2015.

For further discussion around this issue, listen to our podcast.

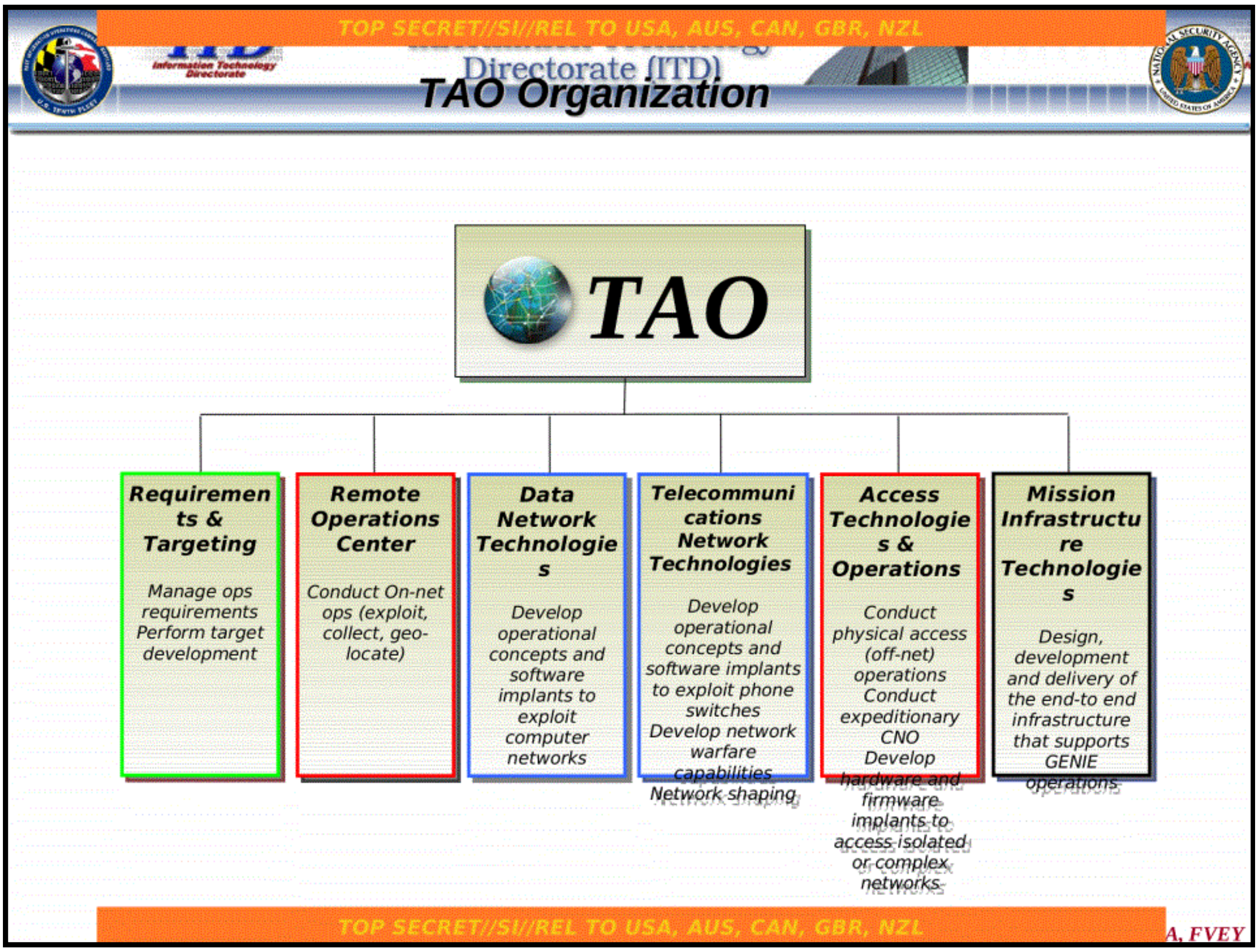
'I fear I've let you all down. Not my intention. I apologize,' lamented George Clooney in an email released to the public as part of a massive cyber-attack on Sony. 'I've just lost touch. Who knew?'

While the attack caused a stir in the entertainment industry, it also has significant implications for the cyber-security landscape. Groups such as Anonymous have long been hacking government agencies, media companies and other targets of their choosing, but the Sony attack is notable for having reportedly been carried out by a state. This poses questions about the capacities of various states to launch attacks over cyberspace, as well as regarding issues of retaliation, proportionality and the absence of rules of engagement.

Although ostensibly conducted by a group calling itself the Guardians of Peace, the FBI has declared that it believes with 'high confidence' that North Korea is ultimately behind the attack, which took place in November 2014. Although this remains contested, North Korea has indeed devoted substantial resources towards enhancing its capacity to operate in cyberspace. According to the testimony of defectors, the North Korean military sent a select group of budding hackers to Beijing in the mid-1990s to be schooled in the art of cyber-war. Soon after they returned, a specialist military intelligence unit dedicated to cyber-operations, Bureau 121, was established; it has since swollen to almost 6,000 people.

Of course, it is not just North Korea that has been pouring resources into improving its cyber capacity. As the United States' signals intelligence agency, the much-maligned National Security Agency (NSA) is responsible for improving the nation's defensive and offensive cyber-capabilities. Much of this work is undertaken by the Office of Tailored

Access Operations (TAO), a highly secretive unit described by a historian as 'akin to the wunderkind of the US intelligence community.'



TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

Information Technology Directorate

Directorate (ITD)

TAO Organization

TAO

Requirements & Targeting
Manage ops requirements
Perform target development

Remote Operations Center
Conduct On-net ops (exploit, collect, geo-locate)

Data Network Technologies
Develop operational concepts and software implants to exploit computer networks

Telecommunications Network Technologies
Develop operational concepts and software implants to exploit phone switches
Develop network warfare capabilities
Network shaping

Access Technologies & Operations
Conduct physical access (off-net) operations
Conduct expeditionary CNO
Develop hardware and firmware implants to access isolated or complex networks

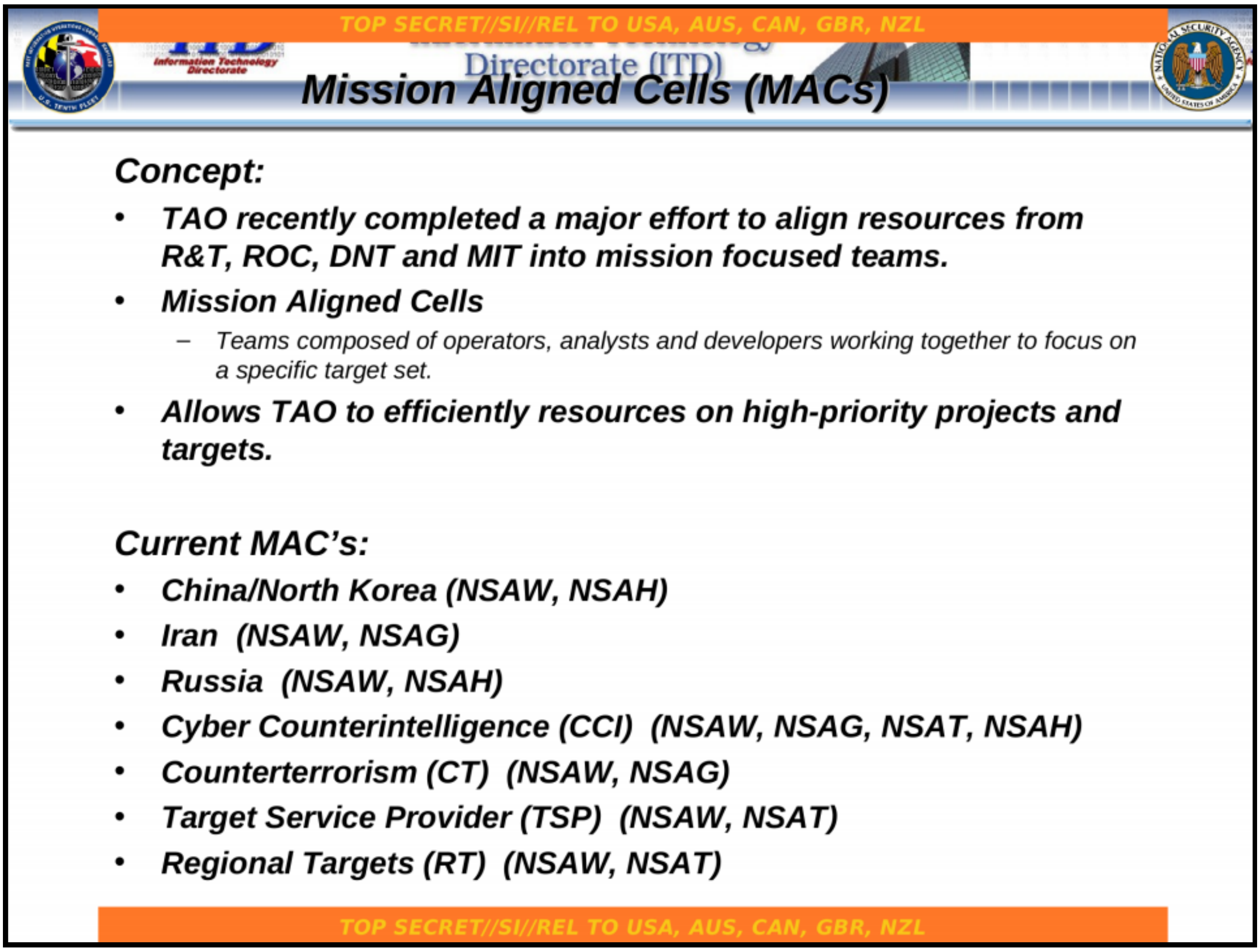
Mission Infrastructure Technologies
Design, development and delivery of the end-to end infrastructure that supports GENIE operations

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

A, FVEY

Figure 1: Extract from NSA training material on Computer Network Operations, released by Edward Snowden, outlining the organisational structure of TAO. Source: Der Spiegel

Analysts, developers and operators within TAO work together in 'Mission Aligned Cells' (MACs), directing their combined expertise towards specific projects. These include traditional intelligence concerns such as 'Counterterrorism' and 'Cyber Counterintelligence' as well as regional cells focusing on areas of interest such as Iran, Russia, and, of course, China/North Korea. Indeed, the most convincing and as yet unreleased evidence linking North Korea to the Sony attacks almost certainly emerged from an NSA operation targeting the country back in 2010.



TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

Mission Aligned Cells (MACs)

Concept:

- TAO recently completed a major effort to align resources from R&T, ROC, DNT and MIT into mission focused teams.
- Mission Aligned Cells
  - Teams composed of operators, analysts and developers working together to focus on a specific target set.
- Allows TAO to efficiently resources on high-priority projects and targets.

Current MAC's:

- China/North Korea (NSAW, NSAH)
- Iran (NSAW, NSAG)
- Russia (NSAW, NSAH)
- Cyber Counterintelligence (CCI) (NSAW, NSAG, NSAT, NSAH)
- Counterterrorism (CT) (NSAW, NSAG)
- Target Service Provider (TSP) (NSAW, NSAT)
- Regional Targets (RT) (NSAW, NSAT)

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

Figure 2: The developers create software and hardware, the analysts in R&T plan the operations, and the operators in ROC conduct the actual intelligence collection. Source: Der Spiegel

The war on Terabytes

In the aftermath of the Sony attack, there has been some discussion as to how to classify it. While some, most notably Republican Senator and presidential fall-short John McCain, have decried the attack as 'a new form of warfare', most agree that it is a 'despicable, criminal act', or, in President Obama's phrasing, simply 'cyber-vandalism'. The lines are becoming increasingly blurred, however. Mr Obama noted that if 'a dictator in another country… disrupt[s]… a company's distribution chain or its products', the US will 'respond proportionately.'

The principle of proportionality is an accepted concept in the laws of war, defined in the Geneva Conventions and elsewhere. But there are no treaties, conventions, precedents or established rules of engagement which govern attacks in cyberspace. This legal vacuum will prove problematic when cyber-weapons not only cause substantial disruption, destruction, and damage but also have lethal effects.

Such a scenario is not difficult to imagine. In our modern, hyper-connected world where even our toasters are connected to the 'internet of things', critical national infrastructure such as power grids, transport networks and financial systems are spectacularly vulnerable to cyber-attack. A successful attack on the City of London or Wall Street could have devastating effects on the nation's economy.

Perhaps the most well-known and most destructive cyber-attack to date was Stuxnet, a highly sophisticated cyber-weapon which attacked Iran's Natanz nuclear facility and widely believed to have been designed and unleashed by the US and Israeli governments. As well as destroying up to a fifth of the centrifuges – over 1,000 – in the Natanz facility, the worm also unintentionally infected over 60,000 computer systems in the US, UK, Australia, Germany and elsewhere.

If the Sony attack was only cyber-vandalism, Stuxnet is a step closer to an act of war. While the US response to North Korea comprised further economic sanctions targeting the country's remaining links to the international financial system, Washington is prepared to use force in response to cyber-attacks. The White House International Strategy for Cyberspace notes that 'the United States will respond to hostile acts in cyberspace as we would to any other threat to our country' through 'all necessary means', whether 'diplomatic, informational, military, [or] economic'.

No cyber-weapon as yet has caused lethal damage, and force has never been used in response. But this is unlikely to remain the case forever. The Sony attack, if nothing else, serves as a timely reminder that there is a real threat that information or even infrastructure may be compromised as part of a cyber-attack. It would be prudent to establish international conventions governing the rules of engagement in cyberspace before such a threat is realised.